CLAIMS

What is claimed is:

1. A method for secure key authentication, the method comprising:

generating at a first location a digital signature of a secure key to obtain a digitally signed secure key; and

transmitting the digitally signed secure key from the first location.

2. The method according to claim 1, further comprising generating the digital signature from at least one of an asymmetric encryption algorithm and a symmetric encryption algorithm.

3 The method according to claim 1, further comprising encrypting the digitally signed secure key prior to transmission to obtain an encrypted digitally signed key.

4. The method according to claim 3, wherein the secure key comprises at least one of a master key, a work key and a scrambling key.

5. The method according to claim 4, further comprising:

receiving the digitally signed secure key at a second location; and

decrypting the digitally signed secure key to obtain a decrypted digitally signed secure key.

6. The method according to claim 5, wherein if the secure key comprises a work key then a decrypted digitally signed master key at the second location is utilized for decrypting an encrypted digitally signed work key.

7. The method according to claim 5, wherein if the secure key comprises a scrambling key then a decrypted digitally signed work key at the second location is utilized for decrypting an encrypted digitally signed scrambling key.

8. The method according to claim 5, further comprising verifying authenticity of the digital signature of the digitally signed secure key.

9. The method according to claim 8, further comprising verifying the authenticity of the digital signature utilizing at least one of an asymmetric decryption algorithm and a symmetric decryption algorithm.

10. The method according to claim 8, further comprising determining whether to verify authenticity of the digital signature.

11. A machine-readable storage having stored thereon, a computer program having at least one code section for secure key authentication, the at least one code section being executable by a machine for causing the machine to perform steps comprising:

generating at a first location a digital signature of a secure key to obtain a digitally signed secure key; and

transmitting the digitally signed secure key from the first location.

12. The machine-readable storage according to claim 11, further comprising code for generating the digital signature from at least one of an asymmetric encryption algorithm and a symmetric encryption algorithm.

13 The machine-readable storage according to claim 11, further comprising code for encrypting the digitally signed secure key prior to transmission to obtain an encrypted digitally signed key.

14. The machine-readable storage according to claim 13, wherein the secure key comprises at least one of a master key, a work key and a scrambling key.

15. The machine-readable storage according to claim 14, further comprising:

code for receiving the digitally signed secure key at a second location; and

code for decrypting the digitally signed secure key to obtain a decrypted digitally signed secure key.

16. The machine-readable storage according to claim 15, wherein if the secure key comprises a work key then a decrypted digitally signed master key at the second location is utilized for decrypting an encrypted digitally signed work key.

17. The machine-readable storage according to claim 15, wherein if the secure key comprises a scrambling key then a decrypted digitally signed work key at the second location is utilized for decrypting an encrypted digitally signed scrambling key.

18. The machine-readable storage according to claim 15, further comprising code for verifying authenticity of the digital signature of the digitally signed secure key.

19. The machine-readable storage according to claim 18, further comprising code for verifying the authenticity of the digital signature utilizing at least one of an asymmetric decryption algorithm and a symmetric decryption algorithm.

20. The machine-readable storage according to claim 18, further comprising code for determining whether to verify authenticity of the digital signature.

21. A system for secure key authentication, the system comprising:

at least one processor for generating at a first location a digital signature of a secure key to obtain a digitally signed secure key; and

the at least one processor transmitting the digitally signed secure key from the first location.

22. The system according to claim 21, the at least one processor generating the digital signature from at least one of an asymmetric encryption algorithm and a symmetric encryption algorithm.

23 The system according to claim 21, the at least one processor encrypting the digitally signed secure key prior to transmission to obtain an encrypted digitally signed key.

24. The system according to claim 23, wherein the secure key comprises at least one of a master key, a work key and a scrambling key.

25. The system according to claim 24, the at least one processor:

receiving the digitally signed secure key at a second location; and

decrypting the digitally signed secure key to obtain a decrypted digitally signed secure key.

26. The system according to claim 25, wherein a decrypted digitally signed master key at the second location is utilized for decrypting an encrypted digitally signed work key.

27. The system according to claim 25, wherein a decrypted digitally signed work key at the second location is utilized for decrypting an encrypted digitally signed scrambling key.

28. The system according to claim 25, the at least one processor verifying authenticity of the digital signature of the digitally signed secure key.

29. The system according to claim 28, the at least one processor verifying the authenticity of the digital signature utilizing at least one of an asymmetric decryption algorithm and a symmetric decryption algorithm.

30. The system according to claim 28, the at least one processor determining whether to verify authenticity of the digital signature.

31. The system according to claim 21, wherein the at least one processor comprises at least one of a host processor, a microprocessor, and a microcontroller.

32. A system for secure key authentication, the system comprising:

a transmitter;

the transmitter comprises a generator that generates a digital signature of a secure key to obtain a digitally signed secure key; and

the transmitter transmits the digitally signed secure key.

33. The system according to claim 32, wherein the generator generates the digital signature from at least one of an asymmetric encryption algorithm and a symmetric encryption algorithm.

34 The system according to claim 32, further comprising an encryptor that encrypts the digitally signed secure key prior to transmission to obtain an encrypted digitally signed key.

35. The system according to claim 34, wherein the secure key comprises at least one of a master key, a work key and a scrambling key.

36. The system according to claim 35, further comprising:

a receiver that receives the digitally signed secure key; and

the receiver comprising a decryptor that decrypts the digitally signed secure key to obtain a decrypted digitally signed secure key.

37. The system according to claim 36, wherein the receiver comprises a decryptor that utilizes a digitally signed master key to decrypt an encrypted digitally signed work key.

38. The system according to claim 36, wherein the decryptor utilizes a decrypted digitally signed work key to decrypt an encrypted digitally signed scrambling key.

39. The system according to claim 36, the receiver comprises a verifier that verifies authenticity of the digital signature of the digitally signed secure key.

40. The system according to claim 39, wherein the verifier utilizes at least one of an asymmetric decryption algorithm and a symmetric decryption algorithm.

41. The system according to claim 39, wherein the verifier determines whether to verify authenticity of the digital signature.